UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/597,864	08/10/2006	Rolf Blom	P18376-US1	7275

27045 7590 09/16/2010

ERICSSON INC.
6300 LEGACY DRIVE
M/S EVR 1-C-11
PLANO, TX 75024

EXAMINER	
ZIA, SYED	

ART UNIT	PAPER NUMBER
2431	

NOTIFICATION DATE	DELIVERY MODE
09/16/2010	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

kara.coffman@ericsson.com
jennifer.hardin@ericsson.com
melissa.rhea@ericsson.com

Office Action Summary	Application No.	Applicant(s)	
	10/597,864	BLOM ET AL.	
	Examiner	Art Unit	
	SYED ZIA	2431	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *01 July 2010*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *30-58* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *30-58* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

This office action is in response to remarks filed July 1, 2010. Claims 30-58 are pending.

Response to Arguments

Applicant's arguments filed on July 1, 2010 have been fully considered but they are not persuasive because of the following reasons:

Regarding Claims 1 applicants argued that the cited prior arts (CPA) [Yamaguchi et al. (U. S. Patent No.: 5,604,807)] "*Although Yamaguchi does describe use of a session key, it does not appear that it teaches a session key that is a function of a freshness token. And also does not have no teaching of a freshness token that comprises a random challenge*".

This is not found persuasive. The system of cited prior art teaches a system and method that has code gateway between server and network which receives session key from key delivery centre and shares it with client. The code communication system consists of multiple server and client connected to a delivery centre through a network. The key delivery centre generates a session key. The session key is used to establish a session to provide communication between the client and server. Before a session is established, the client outputs a code communication demand to a code gateway. The code gateway first receives the session key from the key delivery centre. A first gateway session key delivery section and a second gateway session key delivery section delivers this session key to the client. The session key is decoded in a second encipher-decoder in the code gateway. A session key acquisition section receives the session key from the code

gateway. The received session key is stored in a session key holder. A synchronizing establishment unit establishes code synchronisation with the code gateway. A first session establishment section starts a first session with the server. Code synchronization with the server is also performed during this session. A second session establishment unit establishes a second session and a code communication is performed.

As a result, the system of cited prior art does implement and teaches a system and method that relates to inter-network domain key management in communications systems, (Fig.11-13, and col.10 line 35 to col.13 line 35).

Applicants clearly have failed to explicitly identify specific claim limitations, which would define a patentable distinction over prior arts.

Therefore, the examiner asserts that cited prior art does teach or suggest the subject matter broadly recited in independent Claims and in subsequent dependent Claims. Accordingly, rejections for claims 30-58 are respectfully maintained.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

Claims 30-58 are rejected under 35 U.S.C. 102(e) as being anticipated by Yamaguchi et al. (U. S. Patent No.: 5,604,807).

1. Regarding Claim 30, Yamaguchi teach and describes a method of establishing a session key shared between a first network element of a first network domain and a second network element of a second network domain, said first network domain comprising first cryptographic means and means for sharing a secret key with said second network domain comprising second cryptographic means, said method comprising the steps of: said first cryptographic means generating a freshness token; said first cryptographic means generating said session key based on said shared secret key and said generated freshness token; providing said session key (K) to said first network element; providing said freshness token to said second cryptographic means; said second cryptographic means generating a copy of said session key based on said shared secret key and said provided freshness token; and, providing said copy of said session key to said second network element (Fig.11-13, and col.10 line 35 to col.13 line 35).

2. Regarding Claim 31, Yamaguchi teach and describes a method of enabling secure communication between a first network element of a first network domain and a second network element of a second network domain, said first network domain comprising first cryptographic means and means for sharing a secret key with said second network domain comprising second cryptographic means, said method comprising the steps of: said first cryptographic means generating a freshness token; said first cryptographic means generating said session key based on said shared secret key and said generated freshness token; providing said session key to said first network element; providing said freshness token to said second cryptographic means; said second cryptographic means generating a copy of said session key based on said shared secret key and said provided freshness token; providing said copy of said session key to said second

network element; and, said first network element and said second network element securely communicating based on said session key and said copy of said session key (Fig.11-13, and col.10 line 35 to col.13 line 35).

3. Regarding Claim 42, Yamaguchi teach and describes a system of establishing a session key shared between a first network element of a first network domain and a second network element of a second network domain, said first network domain sharing a secret key with said second network domain, wherein said first network domain comprises: first cryptographic means for generating a freshness token and for generating a session key based on said shared secret key and said generated freshness token; means for providing said session key from said first cryptographic means to said first network element; and, means for providing said freshness token to said second network domain; wherein said second network domain comprises: second cryptographic means for generating a copy of said session key based on said shared secret key and said provided freshness token; and, means for providing said copy of said session key from said second cryptographic means to said second network element (Fig.11-13, and col.10 line 35 to col.13line 35).

4. Regarding Claim 43, Yamaguchi teach and describes a system of enabling secure communication between a first network element of a first network domain and a second network element of a second network domain, said first network domain sharing a secret key with said second network domain, wherein said first network domain comprises: first cryptographic means for generating a freshness token and for generating a session key based on said shared secret key

and said generated freshness token; means for providing said session key from said first cryptographic means to said first network element; and, means for providing said freshness token to said second network domain; said second network domain comprises: second cryptographic means for generating a copy of said session key based on said shared secret key and said provided freshness token; and, means for providing said copy of said session key from said second cryptographic means to said second network element, said first network element comprises means for conducting secure communication with said second network element based said session key and said second network element comprises means for conducting secure communication with said first network element based on said copy of said session key (Fig.11-13, and col.10 line 35 tocol.13 line 35).

5. Regarding Claim 51, Yamaguchi teach and describes a network domain comprising: a first network element adapted for communication with a second network element of an external network domain, wherein said network domain and said external network domain sharing a secret key; cryptographic means for generating a freshness token and for generating a session key based on said shared secret key and said generated freshness token; means for providing said session key from said cryptographic means to said first network element; and, means for providing said freshness token to said external network domain, wherein said external network domain comprises means for generating a copy of said session key for said second network element based on said shared secret key and said provided freshness token (Fig.11-13, and col.10 line 35 tocol.13 line 35).

6. Regarding Claim 55, Yamaguchi teach and describes a network domain comprising: a first network element adapted for communication with a second network element of an external network domain, wherein said network domain and said external network domain sharing a secret key; cryptographic means for generating a session key based on said shared secret key and a freshness token provided from said external network domain; and, means for providing said session key from said cryptographic means to said first network element, wherein said external network domain comprises means for generating said freshness token and for generating a copy of said session key for said second network element based on said shared secret key and said generated freshness token (Fig.11-13, and col.10 line 35 to col.13 line 35).

5. Claims 32-41, 44-50, 52-54, and 56-58 are rejected applied as above rejecting Claim 30-31, 42-43, 51 and 55. Furthermore, Yamaguchi teaches and describes a system and method establishing a session key shared between a first network element of a first network domain and a second network element of a second network domain, said first network domain sharing a secret key with said second network domain, wherein said first network domain comprises, wherein,

As per Claim 32, said session key providing step comprises the step of securely providing said session key to said first network element and said session key copy providing step comprises the step of securely providing said copy of said session key to said second network element (col.10 line 35 to col.11 line 50).

As per Claim 33, said freshness token comprises a random challenge and said method further comprises the steps of: said first cryptographic means generating an expected response

based on said shared secret key and said random challenge; providing said expected response to said first network element; said second cryptographic means generating a response based on said shared secret key and said provided random challenge; providing said response to said first network element; and, said first network element authenticating said second network element based on a comparison between said expected response and said response (col.10 line 35 to col.11 line 50).

As per Claim 34, said first cryptographic means comprises an Authentication and Key Agreement (AKA) algorithm for generating said random challenge, said expected response and said session key, and said second cryptographic means comprises an AKA algorithm for generating said response and said copy of said session key (col.11 line 51 to col.13 line 35).

As per Claim 35, further comprising the steps of: said first network element providing an identifier associated with said second network domain to said first cryptographic means; and, said second network element providing an identifier associated with said first network domain to said second cryptographic means (col.11 line 51 to col.13 line 35)..

As per Claim 36, said session key and said copy of said session key are generated based on at least one of said identifier associated with said first network domain and said identifier associated with said second network domain (col.11 line 51 to col.13 line 35).

As per Claim 37, further comprising the steps of: said first cryptographic means identifying said shared secret key based on said identifier associated with said second network domain; and, said second cryptographic means identifying said shared secret key based on said identifier associated with said first network domain (col.11 line 51 to col.13 line 35)..

As per Claim 38, said first cryptographic means is an Authentication, Authorization and Accounting (AAA) server provided in a network node of said first network domain and said second cryptographic means is an AAA server provided in a network node of said second network domain (col.11 line 51 to col.13 line 35).

As per Claim 39, said first network domain shares a second secret key with a third network domain comprising third cryptographic means and at least a third network element (Fig.11-13, and col.10 line 35 to col.13line 35).

As per Claim 40, said first network domain is managed by a first communications network operator and said second network domain is managed by a second different communications network operator (col.10 line 35 to col.11 line 50).

As per Claim 41, further comprising the step of intermittently replacing said shared secret by a new shared secret by basing a key agreement between said first network domain and said second network domain on said shared secret (col.10 line 35 to col.11 line 50).

As per Claim 44, said session key providing means is adapted for securely providing said session key from said first cryptographic means to said first network element and said session key copy providing means is adapted for securely providing said copy of said session key from said second cryptographic means to said second network element (col.10 line 35 to col.11 line 50).

As per Claim 45, said freshness token comprises a random challenge and said first cryptographic means comprises means for generating an expected response based on said shared secret key and said random challenge and said second cryptographic means comprises means for generating a response based on said shared secret key and said random challenge, said first

network domain comprises means for providing said expected response to said first network element and said second network domain comprises means for providing said response to said first network element, wherein said first network element comprises means for authenticating said second network element based on a comparison between said expected response and said response (Fig.11-13, and col.10 line 35 to col.13line 35).

As per Claim 46, said first cryptographic means comprises an Authentication and Key Agreement (AKA) algorithm for generating said random challenge, said expected response and said session key, and said second cryptographic means comprises an AKA algorithm for generating said response and said copy of said session key (col.11 line 51 to col.13 line 35)..

As per Claim 47, said first cryptographic means is an Authentication, Authorization and Accounting (AAA) server provided in a network node of said first network domain and said second cryptographic means is an AAA server provided in a network node of said second network domain (col.11 line 51 to col.13 line 35).

As per Claim 48, further comprising a third network domain with third cryptographic means and at least a third network element, said first network domain and said third network domain share a second secret key (col.10 line 35 to col.11 line 50).

As per Claim 49, said first network domain is managed by a first communications network operator and said second network domain is managed by a second different communications network operator (col.10 line 35 to col.11 line 50).

As per Claim 50, further comprising means for intermittently replacing said shared secret by a new shared secret said shared secret replacing means is adapted for replacing said shared

secret based on a key agreement between said first network domain and said second network domain using said shared secret (col.10 line 35 to col.11 line 50).

As per Claim 52, said session key providing means is adapted for securely providing said session key from said cryptographic means to said first network element (col.10 line 35 to col.11 line 50).

As per Claim 53, said freshness token comprises a random challenge and said cryptographic means comprises means for generating an expected response based on said shared secret key and said random challenge and said external network domain comprises means for generating a response based on said shared secret key and said random challenge, said network domain comprises means for providing said expected response to said first network element and said external network domain comprises means for providing said response to said first network element, wherein said first network element comprises means for authenticating said second network element based on a comparison between said expected response and said response (Fig.11-13, and col.10 line 35 to col.13line 35).

As per Claim 54, said cryptographic means is an Authentication, Authorization and Accounting (AAA) server provided in a network node of said network domain (col.11 line 51 to col.13line 35)..

As per Claim 56, said session key providing means is adapted for securely providing said session key from said cryptographic means to said first network element (Fig.11-13, and col.10 line 35 to col.13line 35).

As per Claim 57, said freshness token comprises a random challenge and said cryptographic means comprises means for generating a response based on said shared secret key

and said random challenge and said external network domain comprises means for generating an expected response based on said shared secret key and said random challenge and means for providing said expected response to said second network element, said network domain comprises means for providing said response to said second network element, wherein said response and said expected response enables said second network element to authenticate said first network element (Fig.11-13, and col.10 line 35 to col.13line 35).

As per Claim 58, said cryptographic means is an Authentication, Authorization and Accounting (AAA) server provided in a network node of said network domain (col.11 line 51 to col.13 line 35).

Conclusion

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37

CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to SYED ZIA whose telephone number is (571)272-3798. The examiner can normally be reached on 9:00 to 5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

sz
September 9, 2010
/Syed Zia/
Primary Examiner, Art Unit 2431